Hervey Allen

Network Startup Resource Center

PacNOG 6: Nadi, Fiji

Dealing with DDoS Attacks

Overview: What is a "DDoS"

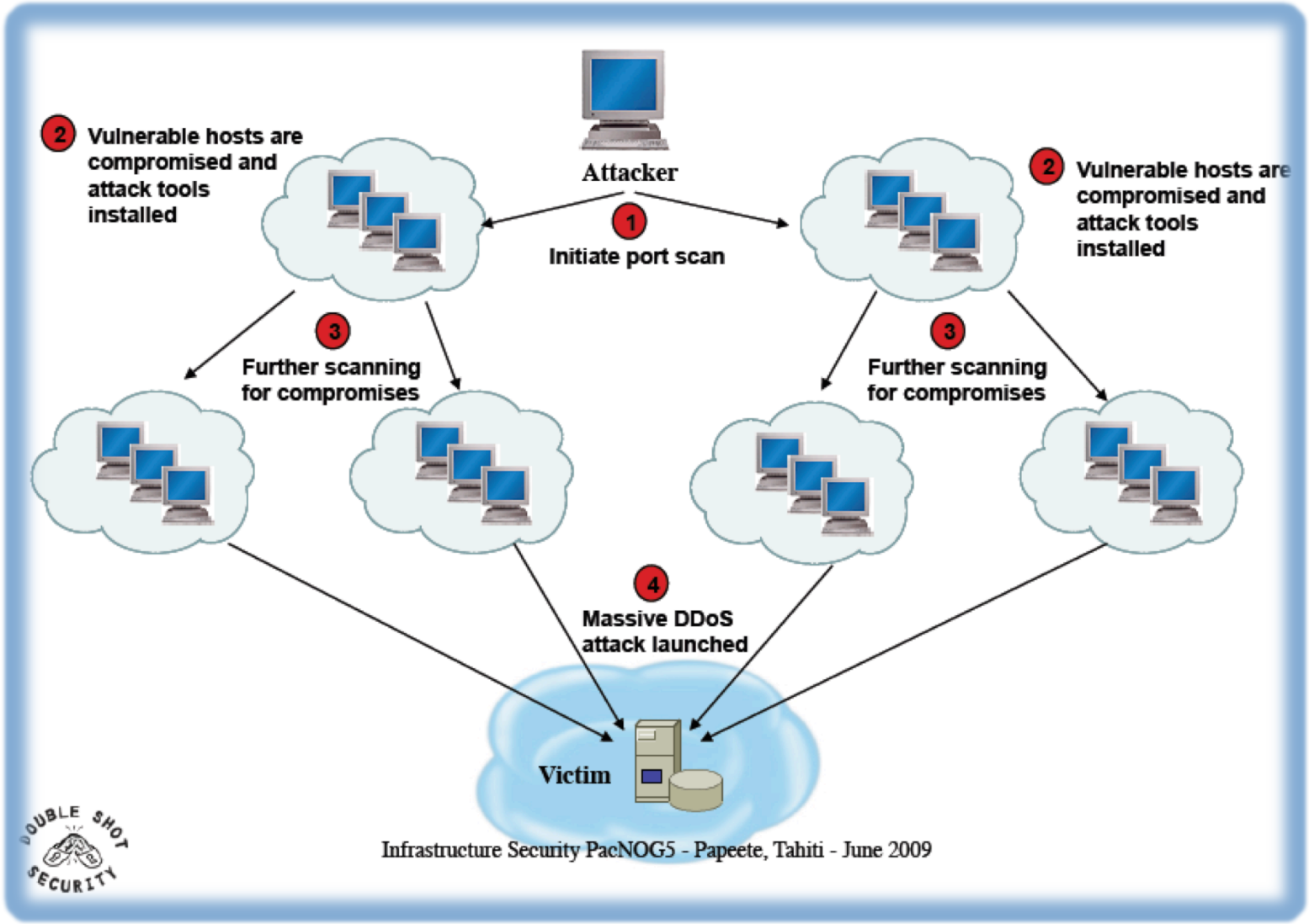
DDoS ➔ "Distributed Denial of Service" Attack

DOS ➔ "Denial of Service" Attack

"A **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a computer resource unavailable to its intended users. It generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely."*

*http://en.wikipedia.org/wiki/DDoS#Distributed_attack

Automated DDoS Attacks



Overview: How to Mitigate DDoS

- Ingress/Egress filters
- Capacity
- Contingency Response
- Firewalls
- Separation of services
- Monitor traffic flow
- Monitor services
- Monitor your logs

Ingress Filters

See PacNOG5 Network Security Track for details:

http://www.pacnog.org/pacnog5/track3/index.html

RFC2827 (BCP38) – Ingress Filtering

If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.

The ONLY valid source IP address for packets originating from a customer network is the one assigned by the ISP (whether statically or dynamically assigned).

An edge router could check every packet on ingress to ensure the user is not spoofing the source address on the packets which he is originating.

Egress Filters

Deny Broadcast Packets from infected machines.

Add Capacity

- This is expensive!
- Overbuild on network infrastructure:
  - Routers
  - Switches
- Verify servers have extra capacity.

This is what larger organizations are doing today. It's *expensive*. Many of you are temporarily "protected" from DDoS due to incoming network bandwidth.

Contingency Response

- Have a plan ☺
- Know who to call
  - Do you have the technical contacts for your upstream provider?
  - Your technicians. Do you have a way to contact them during off-hours.
- Which services are critical. Can others be dropped? Turned off?
- Can you temporarily add capacity if necessary?

Firewalls

- In Linux you can use *iptables*:
- Rules are stored in a file. First rule is generally “deny all”

```
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP
```

- Rules look something like…

```
ipfw add deny tcp from evil.doers.org to nice.people.org 22
ipfw add deny log tcp from evil.crackers.org/24 to nice.people.org
```

- Large, in-depth discussion here:

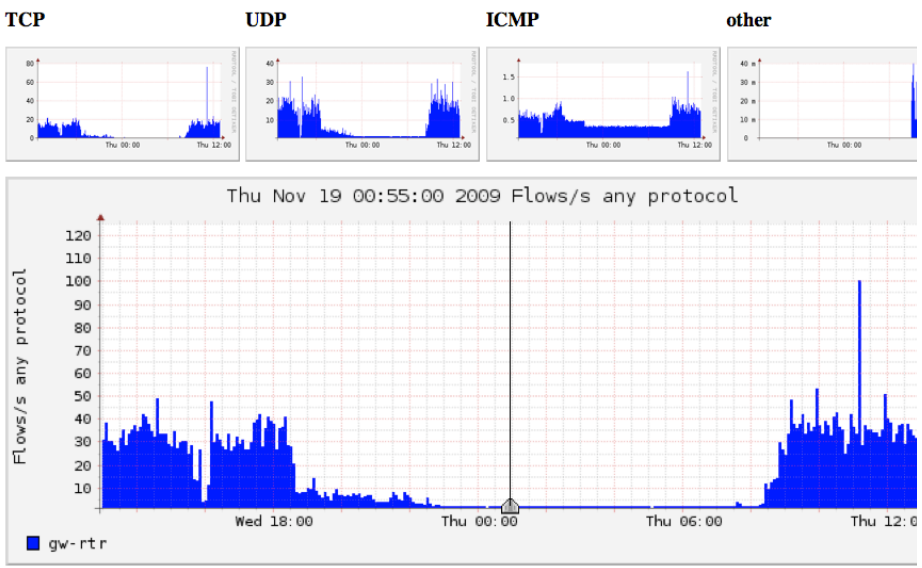
http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html

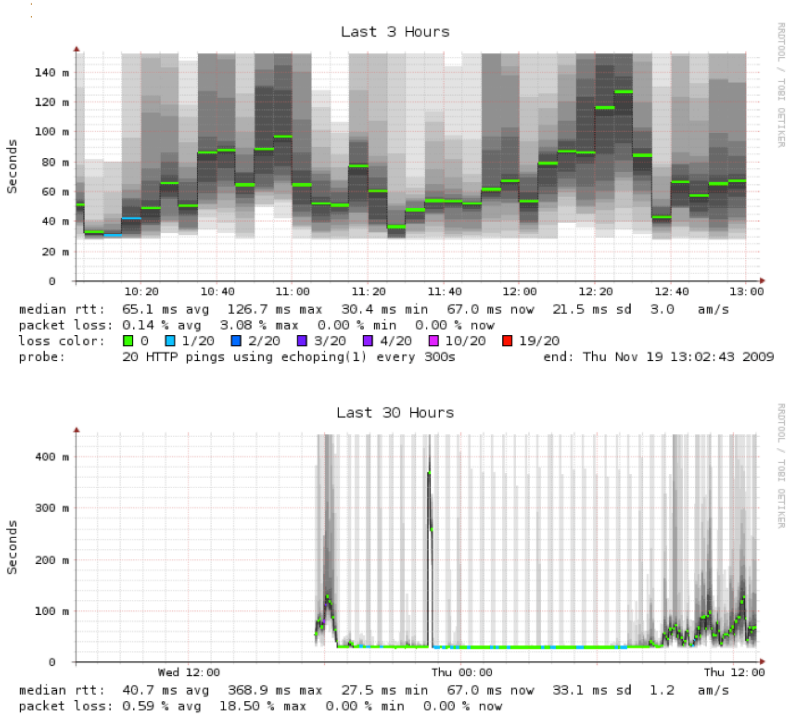
Separation of Services

- Often services are targeted, such as:
  - web
  - dns
  - ftp
  - mail
- Try to place these on separate machines.
- Or, move a service to another machine if necessary.
- Place services on different parts of your network (other IP address ranges…)

Monitor Traffic Flow

- Using tools like Netflow, NfSen, Smokeping, etc.
- Configure alarms for traffic thresholds.





Monitor Services

- Lots and lots of tools for this.
- Nagios, Cacti, Smokeping we've seen this week.
- Trigger alarms when service degrades.

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
0.ge-0-1-0.uonet8-gw.uoregon.edu	PING	OK	11-18-2009 17:04:12	60d 12h 18m 1s	1/3	PING OK - Packet loss = 0%, RTA = 0.49 ms
afnog.org	HTTP	OK	11-18-2009 17:04:21	1d 22h 9m 48s	1/3	HTTP OK HTTP/1.1 200 OK - 13875 bytes in 1.652 seconds
	PING	OK	11-18-2009 17:07:35	0d 10h 46m 34s	1/3	PING OK - Packet loss = 0%, RTA = 335.54 ms
	SMTP	OK	11-18-2009 17:12:19	12d 12h 17m 29s	1/3	SMTP OK - 1.714 sec. response time
	SSH	OK	11-18-2009 17:05:36	14d 5h 38m 33s	1/3	SSH OK - OpenSSH_5.1p1 FreeBSD-20080901 (protocol 2.0)
limestone.uoregon.edu	HTTP	OK	11-18-2009 17:12:25	25d 12h 51m 44s	1/3	HTTP OK HTTP/1.1 200 OK - 1114 bytes in 5.485 seconds
	PING	OK	11-18-2009 17:10:04	219d 7h 45m 39s	1/3	PING OK - Packet loss = 0%, RTA = 0.09 ms
	SSH	OK	11-18-2009 17:08:29	15d 22h 33m 11s	1/3	SSH OK - OpenSSH_4.3 (protocol 2.0)
nsrc.org	Current Load	OK	11-18-2009 17:09:30	210d 2h 34m 9s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	11-18-2009 17:09:27	258d 10h 25m 4s	1/4	USERS OK - 0 users currently logged in
	HTTP	OK	11-18-2009 17:12:13	5d 10h 6m 31s	1/4	HTTP OK HTTP/1.1 200 OK - 17594 bytes in 0.001 seconds
	PING	OK	11-18-2009 17:13:47	219d 7h 52m 12s	1/4	PING OK - Packet loss = 0%, RTA = 0.01 ms
	Root Partition	OK	11-18-2009 17:09:30	258d 10h 23m 12s	1/4	DISK OK - free space: / 2569892 MB (95% inode=99%):
	SSH	OK	11-18-2009 17:09:21	219d 7h 52m 11s	1/4	SSH OK - OpenSSH_5.1p1 Debian-5ubuntu1 (protocol 2.0)

Monitor Logs

- We just learned about this!
- Be sure you do it!
- Swatch, syslog, syslog-ng, etc.
- Monitor your log file sizes. You can do this with Cacti, Nagios, scripts.
- Use your logs for forensic research:

```
$ sudo grep ssh /var/log/messages | less
```